AMENDMENT

In the Claims

Please cancel Claims 1-40 and add Claims 41-70 as shown below.

1-40. (canceled)

41. (new) A method for remotely monitoring each of a plurality of intrusion protection devices with a remote monitoring center under control by a service provider servicing the intrusion protection requirements of a plurality of customers, wherein the remote monitoring center operates at a location other than a site of any one of the customers, comprising the steps of:

receiving at the remote monitoring center a first transmission comprising a first identification number and a network address associated with one of a plurality of communication devices monitored by the remote monitoring center, each communication device positioned in-line with a computer network controlled by one of the customers and a distributed computer network that is not controlled by the customers, each communication device operative to block a communication from passing to the corresponding computer network via the distributed computer network by terminating the communication based on a determination that the communication represents a security risk to at least one of the computers coupled to the computer network;

storing the identification number and network address for the communication device in a database at the remote monitoring center;

receiving at the remote monitoring center a second identification number during a second transmission from the communication device;

comparing the second identification number with the first identification number at the remote monitoring center and, in response to a match between the first identification number and second identification number, identifying a plurality of security policy options that are selectable by the communication device;

generating a configuration file with the remote monitoring center in response to selection of at least one of the security policy options by the communication device, the configuration file governing the intrusion protection operation for the communication device;

transmitting the configuration file from the remote monitoring center to configure the communication device;

monitoring the communication device by the remote monitoring center for issuance of an alert signal issued by the communication device in response to a determination that the communication represents a security risk to at least one of the computers coupled to the computer network;

receiving the alert signal at the remote monitoring center; and

assigning the alert signal an order and taking responsive action at the remote monitoring center based upon the assigned order.

42. (new) The method of claim 41, further comprising the step of storing the alert signal into another database connected to the remote monitoring center, wherein servicing the protection requirements of a plurality of customers comprises monitoring each of the plurality of communication devices for generation of the alert signal.

43. (new) The method of claim 41, further comprising the step of:

receiving at the remote monitoring center status information from one of the communication devices;

recording the status information in the database; and

determining whether the communication device meets a plurality of operational requirements based upon the status information.

44. (new) The method of claim 41, further comprising the steps of:

receiving at the remote monitoring center a plurality of diagnostic variables from one of the communication devices; and

determining whether the communication device is functioning properly based on the diagnostic variables.

45. (new) The method of claim 41, further comprising the steps of:

receiving at the remote monitoring center status information from one of the communication devices;

determining whether the communication device requires a software patch based upon the status information; and

transmitting the software patch to the communication device in response to determining the communication device requires the software patch.

46. (new) The method of claim 41, further comprising the steps of:

receiving at the remote monitoring center a configuration complete signal;

performing a vulnerability analysis on one of the communication devices; and

evaluating the results of the vulnerability analysis.

47. (new) A method for remotely monitoring a plurality of communication devices based on operations of a remote monitoring center managed by a service provider, each communication device positioned in-line with a computer network under control of one of a plurality of customers and a distributed computer network that is not under control of the customers, comprising the steps of:

presenting security policy options with the remote monitoring center, the security policy options selectable by each of the communication devices;

generating a configuration file with the remote monitoring center in response to selection of the security policy options by each of the communication devices;

transmitting the configuration file from the remote monitoring center to configure the communication devices, each communication device operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to a corresponding one of the computer networks to determine whether the communication represents a security risk to the computer network in accordance with the configuration file, the communication device further operative to issue an alert signal and to terminate the communication in response to a determination that the communication represents a security risk;

monitoring the communication devices with the remote monitoring center to detect an issuance of the alert signal from one of the communication devices;

receiving the alert signal with the remote monitoring center; and

forwarding the alert signal to a remote agent associated with the service provider, wherein the alert signal provides an advisory of the security risk faced by the communication device that issued the alert signal.

48. (new) The method of claim 47, further comprising the steps of:

assigning a priority to the alert signal upon receipt of the alert signal at the remote monitoring center; and

forwarding the alert signal to the remote agent according to the assigned priority.

49. (new) The method of claim 47, further comprising the steps of:

receiving the alert signal with the remote agent;

determining an appropriate resolution to address the alert signal; and

sending a message comprising the resolution to a particular one of the customers associated with the communication device that issued the alert signal.

50. (new) The method of claim 47, further comprising the steps of:

prior to displaying security policy options, receiving a wake-up signal from one of the communication devices at the remote monitoring center; and

in response to the wake-up signal, transmitting the configuration file from the remote monitoring center to the communication device.

a1

51. (new) The method of claim 47, further comprising the step of:

receiving a first identification number and a network address at the remote monitoring center from one of the communication devices; and

recording the first identification number and the network address in a database connected to the remote monitoring center.

52. (new) The method of claim 47, further comprising the step of:

receiving at the remote monitoring center status information from one of the communication devices;

recording the status information in a database; and

determining whether the communication device meets a plurality of operational requirements based upon the status information.

53. (new) The method of claim 47, further comprising the steps of:

receiving at the remote monitoring center a plurality of diagnostic variables from one of the communication devices; and

determining whether the communication device is functioning properly based on the diagnostic variables.

54. (new) The method of claim 47, further comprising the steps of:

receiving at the remote monitoring center status information from one of the communication devices;

a1 determining whether the communication device requires a software patch based upon the status information; and

transmitting the software patch to the communication device in response to determining that the communication device requires the software patch.

55. (new) The method of claim 47, further comprising the steps of:

responsive to configuration of one of the communication devices, performing a vulnerability analysis for the communication device; and

determining whether the communication device failed the vulnerability analysis.

56. (new) A method for remotely configuring intrusion protection operations, comprising the steps of:

determining a network address for a communication device positioned in-line between a distributed computer network and a computer network, the communication device operable to provide protection from an attack communication carried by the distributed computer network and intended for transmission to a computer coupled to the computer network;

transmitting from the communication device a wake-up signal comprising the network address via an encrypted communication channel to a remote computer; and

receiving from the remote computer configuration information for the communication device via the encrypted communication channel, the configuration information comprising a security policy that instructs the communication device to block the attack communication in response to a determination by the communication device that the attack communication represents a security risk.

57. (new) The method of claim 56, further comprising the step of receiving at the communication device a software patch from the remote computer.

58. (new) The method of claim 56, further comprising the step of transmitting status information from the communication device to the remote computer.

59. (new) The method of claim 56, further comprising the step of transmitting diagnostic information from the communication device to the remote computer.

60. (new) The method of claim 56, further comprising the step of transmitting a configuration complete signal from the communication device to the remote computer to advise of completed configuration operations at the communication device.

61. (new) A system for remotely monitoring the security status of a plurality of computer networks, each computer network associated with one of a plurality of entities, comprising:

a plurality of communication devices, each communication device coupled in-line with one of the computer networks associated with a particular one of the entities and a distributed computer network that is not associated with any of the entities,

wherein each communication device is operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to the corresponding computer network to determine whether the communication represents a security risk to the computer network, and

a1 wherein each communication device is further operative to block the communication from passage to the computer network by terminating the communication and to transmit an alert signal via the distributed computer network in response to a determination by the communication device that the communication represents a security risk; and

a remote monitoring center operated on behalf of the entities by a service provider, the remote monitoring center coupled to the distributed computer network, remotely located from each of the computer networks, and operative to monitor the security status of each one of the plurality of computer networks based upon status information transmitted by the communication devices for the computer networks, the remote monitoring center responsive to receipt of the alert signal transmitted by any one of the communication devices to complete an analysis of the alert signal and to take a responsive action based on the analysis of the alert signal.

62. (new) The system of Claim 61, wherein the remote monitoring center comprises:

one or more remote agent personnel for evaluating the alert signal;

a database for storing alert information presented by the alert signal;

a server maintaining security configuration options for each of the communication devices;

a controller for permitting access to the communication device security options based upon a comparison of identification information associated with one of communication devices to identification information stored in the database, and for transmitting a configuration file to the communication device in response to a configuration request made by the communication device; and

a monitoring engine for receiving the alert signal and recording information about the alert signal in the database, and for forwarding the alert signal to the one or more remote agent personnel.

63. (new) The system of claim 62, wherein each agent personnel is under control of the service provider while each communication device is under control of one of the entities subscribing to a network security monitoring service sponsored by the service provider.

64. (new) The system of claim 62, wherein one of the agent personnel recommends a responsive action to take in reply to the alert signal, the responsive action presented to the entity associated with the communication device that issued the alert signal, the responsive action delivered via one of a Web server, an e-mail message, a telephone, and a pager.

65. (new) The system of claim 61, wherein each communication device comprises:

an intrusion detector, positioned between the computer network and the distributed computer network, for receiving the communication from the distributed computer network and processing the communication to determine whether the communication represents a security risk;

a processor operative to determine a network address for the communication device; and

a transmitter for sending the wake-up signal comprising the network address to the remote monitoring center via the distributed computer network, the transmitter further operative to send the alert signal in response to a determination by the intrusion detector that the communication represents a security risk.

66. (new) A remote monitoring center system for remotely monitoring the security status of a plurality of computer networks, comprising:

one or more workstations operated by remote agent personnel for evaluating an alert signal issued by one of a plurality of communication devices, each communication device coupled in-line with one of the computer networks associated with a particular one of the entities and a distributed computer network, the communication device operative to block a communication from passage to the computer network by terminating the communication and to transmit the alert signal via the distributed computer network in response to a determination that the communication represents a security risk;

a database for storing alert information presented by the alert signal;

a server maintaining security configuration options for each communication device;

a controller for receiving a wake-up signal from each communication device, for permitting access to the communication device security options based upon a comparison of identification information associated with the communication device to identification information stored in the database, for receiving a configuration request from the communication device, and for transmitting a configuration file to the communication device in response to a configuration request made by the communication device; and

a monitoring engine for receiving the alert signal issued by the communication device and recording information about the alert signal in the database, and for forwarding the alert signal to the one or more remote agent personnel.

67. (new) A communication device for intrusion protection, coupled in-line with a computer network under control of a user and a distributed computer network that is not under control of the user, comprising

an intrusion processor, coupled in-line with the computer network and the distributed computer network, for processing a communication carried by the distributed computer network and intended for delivery to a computer coupled to the computer network to determine whether the communication represents a security risk to the computer network, the intrusion processor operative to block the communication from passage to the computer network by terminating the communication in response to a determination that the communication represents a security risk;

an processing module operative to determine a network address for the communication device; and

a transmitter, coupled to the distributed computer network and to the processing module, for sending a wake-up signal comprising the network address to a remote monitoring center coupled to the distributed computer network, the transmitter further operative to send an alert signal to the remote monitoring center in response to processing operations by the intrusion detector resulting in a determination that the communication represents a security risk.

68. (new) A method for remotely monitoring the security status of a plurality of computer networks, each computer network associated with one of a plurality of entities, comprising:

providing a plurality of communication devices, each communication device coupled in-line with one of the computer networks associated with a particular one of the entities and a distributed computer network, the communication device operative to process a communication carried by the distributed computer network and intended for delivery to a computer coupled to the computer network to determine whether the communication represents a security risk to the computer network, the communication device further operative to block the communication from passage to the computer network by terminating the communication and to transmit an alert signal via the distributed computer network in response to the determination that the communication represents a security risk; and

operating a remote monitoring center, coupled to the distributed computer network and remotely located from each of the computer networks, on behalf of each of the plurality of entities to monitor the security status of each one of the plurality of computer networks based upon status information transmitted by the communication devices associated with the computer networks, the remote monitoring center responsive to receipt of the alert signal transmitted by any one of the communication devices to complete an analysis of the alert signal and to take a responsive action based on the analysis of the alert signal.

69. (new) A method for remotely monitoring the security status of a plurality of computer networks, each computer network associated with one of a plurality of entities and coupled to a distributed computer network, comprising:

for each of the computer networks,

processing a communication carried by the distributed computer network and intended for delivery to a computer coupled to the corresponding computer network to determine whether the communication represents a security risk to the computer network,

blocking the communication from passage to the computer network by terminating the communication in response to a determination that the communication represents a security risk, and

a1 transmitting an alert signal via the distributed computer network in response to terminating the communication to advise of the security risk posed to the computer network; and

on behalf of each of the plurality of entities associated with the computer networks,

monitoring the security status of each one of the plurality of computer networks, and

responsive to receipt of the alert signal, completing an analysis of the alert signal and taking a responsive action based on the analysis of the alert signal.

70. (new) The method of Claim 69, further comprising the step of forwarding the alert signal to a remote agent that is located at a position other than the location of any of the computer networks, the remote agent operative to contact the entity associated with the computer network facing the security risk.

REMARKS

The Applicant and the undersigned thank Examiner Nalven for a careful review of this application. Consideration of the present application is respectfully requested in view of the foregoing amendment and the following remarks, which are responsive to the Official Action mailed September 30, 2003.

With the entry of this amendment, Claims 41-70 are pending in the present application. Without prejudice to, or disclaimer of, the subject matter recited therein, Applicant has canceled Claims 1-40 and reserves the right to seek patent protection for the inventions defined by Claims 1-40 at a later date in view of the patentable aspects of these inventions. Claim 41, 47, 56, 61, 66, 67, 68, and 69 are independent claims. No new matter is added by the entry of the new claims.

In the Official Action, the Examiner rejected Claims 1-40, which Applicant has canceled in this Response, based on the assertion that each of these claims is not patentable over U.S. Patent No. 5,991,881 to Conklin, U.S. Patent No. 6,530,024 to Proctor, E.P.O. Published Patent Application 0,793,170 to Hamilton, U.S. Patent No. 5,956,716 to Kenner, WO Patent Publication 98/26548 to Li, U.S. Patent No. 6,301,668 to Gleichauf, U.S. Patent No. 6,324,692 to Fiske, or U.S. Patent No. 6,012,100 to Frailong, or to an alleged combination of two or more of these patent references. While Applicant respectfully disagrees with the Examiner's characterization of the inventions of Claim 1-40 and the cited prior art, the cancellation of Claims 1-40 precludes the need for Applicant's rebuttal of these issues in this paper.

I. New Independent Claims 41, 47, 56, 61, 66, 67, 68, and 69 are Patentable over the Cited Prior Art

Applicant has added new Claims 41-70, of which Claims 41, 47, 56, 61, 66, 67, 68, and 69 are independent claims, to provide a scope of protection commensurate with the original disclosure. Applicant submits that Claims 41-70 are patentable over and distinguishable from the cited references, either singularly or in combination, and offers the below remarks to highlight select distinctions between new independent Claims 41, 47, 56, 61, 66, 67, 68, and 69 and certain references cited by the Examiner.

A. Independent Claim 41 is Distinguishable from *Proctor* and *Conklin*

New Claim 41 is an independent method claim for remotely monitoring intrusion protection devices with a remote monitoring center that is controlled by a provider of intrusion protection services, wherein the remote monitoring center is located offsite from any of the customers that receive the center's intrusion protection services.

> ***Proctor* and *Conklin* fail to disclose or teach a communication device, positioned in-line with a computer network and a distributed computer network, that blocks a communication representing a security risk by terminating that communication.**

The invention of Claim 41 requires a plurality of communication devices, positioned in-line with a computer network and a distributed computer network, and a remote monitoring center that monitors each of the communication devices. From a position in the line of communication for both networks, the communication device blocks a communication passing to the computer network via the distributed computer network by terminating the communication based on a determination by the device that the communication represents a security risk. An in-line communication device having the features defined by Claim 41 is not disclosed by *Conklin*, *Proctor*, a combination of *Conklin* and *Proctor* or the remaining prior art of record.

In contrast to a communication device with the features recited in Claim 41, *Conklin* teaches positioning a network surveillance device out-of-line with a computer network. See *Conklin* Figures 1-4. In particular, *Conklin* teaches a star configuration of two Ethernet network segments and a terminal network connection leading to a network surveillance device for a computer network. *Conklin* further teaches system configurations in which all communications between two computers on an Ethernet segment are broadcast on the Ethernet segment, thus facilitating receipt of broadcast communication signals by an out-of-line surveillance device. See *Conklin* column 2 lines 43-58. *Conklin's* star configuration contrasts with the recited communication device in an in-line configuration with a computer network and a distributed computer network, as defined by Claim 41. See *Conklin* Figure 3.

Whereas Claim 41 recites terminating a communication that represents a security risk, based on an action taken by an in-line device, *Conklin* teaches shadowing an attacker and logging the attacker's activities for evidentiary purposes without interrupting the attacker's

logging the attacker's activities for evidentiary purposes without interrupting the attacker's communications. See *Conklin* column 7 lines 39-43 and column 8 lines 1-5. *Conklin* fails to show blocking a communication carried by a distributed computer network from entering the protected computer network based on actions taken at a communication device placed between the networks.

Like *Conklin*, *Proctor* does not disclose a communication device, in-line between a computer network and a distributed computer network, operative to block a communication representing a security risk by terminating the communication. As opposed to blocking a threatening communication, *Proctor* teaches shutting down a computer that is a target of a threatening communication, logging off a user that is suspected of breaching security, minimizing a suspected user's granted access, updating and implementing security policies, or delaying intervention and recording a suspected user's activities. See *Proctor* column 4 lines 59-62 and column 7 lines 5-26.

While Claim 41 requires the recited communication device to be in-line with a computer network and a distributed computer network, *Proctor* teaches locating a computer that performs network security functions (that do not include blocking a threatening communication) on a network along with the computers that are potential attack targets. See *Proctor* column 5 lines 38-60 and Figure 1. In contrast to the placement of the communication device recited by Claim 41, *Proctor* discloses positioning a computer performing security functions at undisclosed locations in a network environment, characterized as one or more local area networks or wide area networks. See *Proctor* Figure 1 and column 5 lines 4-17.

***Proctor* and *Conklin* fail to disclose or teach a remote monitoring center operating at a location other than a site of any one of the customers serviced by a service provider controlling the monitoring center.**

In contrast to Claim 41, neither *Proctor* nor *Conklin* discloses a single remote monitoring center that remotely monitors a plurality of intrusion protection devices, where the remote monitoring center operates at a location other than a site of any of the customers of a service provider controlling that remote monitoring center. Although *Proctor* may disclose placing elements of a security system on a local area network or a wide area network that is connected to

computers served by the security system, *Proctor* does not teach locating a remote monitoring center offsite from these computers. Instead, *Proctor* teaches locating a security system on a network of computers that are potential targets of a security intrusion to secure protection of network. See *Proctor* Figure 1, column 5 lines 4-17, and column 15 lines 35-39. Further, *Proctor* does not disclose a service provider controlling a remote monitoring center and providing intrusion protection service via a customer relationship. Rather than involving a service provider in network security, *Proctor* teaches managing security with a security administrator, specifically defined as a user, for example a system administrator or a network administrator. See *Proctor* column 3 lines 49-52.

Conklin also fails to disclose remote monitoring of intrusion protection devices by an offsite monitoring center that is controlled by a provider of intrusion protection services. Rather than locating a monitoring center in a remote location with respect to customer computers, as required by Claim 41, *Conklin* teaches integrating centralized security monitoring capabilities into existing network management systems. See *Conklin* column 1 lines 24-26. Furthermore, *Conklin* teaches locating at least a portion of a security monitoring system on an Ethernet network segment using Ethernet hardware and addresses. (Ethernet is generally regarded as a local area network technology.) See *Conklin* column 3 lines 46-49 and Figure 4.

***Proctor* and *Conklin* fail to disclose or teach identifying security options in response to matching identification numbers of received transmission.**

Claim 41 recites identifying a plurality of security options that are selectable by a communication device, which has the recited features discussed above, in response to a match between the identification numbers of two transmissions received at a remote monitoring center. Neither *Conklin* nor *Proctor*, either singularly or in combination, discloses identifying security options in response to matching identification numbers of two transmissions received at a remote monitoring center.

In contrast to matching identification numbers of two transmissions received at a remote monitoring center, *Conklin* teaches matching a packet with a predefined intrusion profile to identify traffic that may be intrusive. See *Conklin* column 5 lines 24-31 and Figure 7. Rather than identifying security options in response to matching transmission identification numbers as

log file. See *Conklin* column 5 lines 32-44. Also, in contrast to matching transmission identification numbers, as required by Claim 41, *Proctor* discloses monitoring activity levels to determine if these levels deviate from normal ranges. Unlike identifying selectable security options in accordance with the recitations of Claim 41, *Proctor* teaches updating security policies in response to detecting threatening security occurrences. See *Proctor* column 14 lines 39-54.

***Proctor* and *Conklin* fail to disclose or teach assigning an order to an alert signal.**

Another recitation that distinguishes Claim 41 from *Conklin* and from *Proctor* is the step of assigning an order to an alert signal and taking responsive action at a remote monitoring center based on the assigned order. Neither *Conklin* nor *Proctor* teaches responding to security threats on an ordered basis or discloses accommodating multiple security threats in a systematic manner. *Proctor* discloses responding to each security incident without considering a response order with respect to another incident. See *Proctor* Abstract. Likewise, *Conklin* teaches initiating a log of activities upon detection of an attempted intrusion without regard to responding before or after another intrusion. See *Conklin* Abstract.

B. Independent Claim 47 is Distinguishable from *Proctor* and *Conklin*

New Claim 47 is an independent method claim for remotely monitoring in-line communication devices based on operations of a remote monitoring center under management of a service provider. The invention of Claim 47 is distinguishable from *Proctor* and *Conklin* by recitations in this claim that are neither taught nor disclosed by either of these cited references.

***Proctor* and *Conklin* fail to disclose or teach an in-line communication device that is operative to communication by terminating the communication in response to a determination that the communication represents a security risk.**

As discussed above in reference to Claim 41, the teachings of *Proctor* and *Conklin* contrast with the recitations in Claim 47 of a communication device, positioned in-line with a computer network under control of customer and a distributed computer network that is not

controlled by the customer, operative to block a communication by terminating the communication in response to a determination that the communication represents a security risk.

Proctor and Conklin fail to disclose or teach remotely monitoring communication devices based on operations of a remote monitoring center managed by a service provider.

As discussed above in reference to Claim 41, neither *Proctor* nor *Conklin* discloses a remote monitoring center, managed by a service provider, that remotely monitors a plurality of communication devices having the operability recited in Claim 47.

***Proctor* and *Conklin* fail to disclose or teach presenting selectable security policy options.**

Claim 47 recites a remote monitoring center presenting security policy options that are selectable by communication devices, each of which is operative to process a communication, determine security risk, and issue an alert. *Proctor* does not disclose presenting security policy options that are selectable by security devices. In contrast to presenting selectable security policy options, *Proctor* discloses updating security policies and alerting a network administrator upon an occurrence of a security incident so the administrator can manually intervene. See *Proctor* column 14 lines 46-63.

Conklin also fails to disclose presenting security policy options that are selectable by security devices, but rather teaches recording communications to acquire intrusion evidence. See *Conklin* column 5 lines 15-21. In further contrast to presenting security policy options that are selectable by security devices, *Conklin* teaches providing system administrators with notification of security events to improve their ability to effectively react to intrusion incidents. See *Conklin* column 7 lines 5-7.

C. Independent Claim 56 is Distinguishable from *Proctor* and *Conklin*

New Claim 56 is an independent claim of a method for remotely configuring intrusion protection operations.

***Conklin* and *Proctor* fail to disclose a method for remotely configuring intrusion protection operations.**

Conklin does not disclose a method for remotely configuring intrusion protection operations, but rather discloses a system recording intrusion activity for evidence that is easily integrated into existing network management systems. See *Conklin* column 1 lines 21-27. *Proctor* also fails to disclose a method for remotely configuring intrusion protection operations. Instead, *Proctor* teaches locating a security system that adapts security procedures on the same network as the computers that are recipients of adapted security procedures. See *Proctor* Figure 1 and column 2 lines 51-55.

***Conklin* and *Proctor* fail to disclose instructing a communication device to block an attack communication.**

Another distinguishing feature between Claim 56 and *Conklin* and *Proctor* is the step of instructing a communication device to block an attack communication in response to a determination that the attack communication represents a security risk. Neither *Conklin* nor *Proctor* discloses blocking an attack communication with a communication device. In contrast to instructing a communication device to block an attack communication, *Conklin* discloses notifying a system administrator of an intrusion event so this administrator can react. See *Conklin* column 7 lines 5-7. Also, in contrast to this blocking step in Claim 56, *Proctor* teaches shutting down a computer that is under attack, logging off suspected attacker, or minimizing a suspected attacker's access in response to an intrusion event. See *Proctor* column 7 lines 5-14.

***Conklin* and *Proctor* fail to disclose transmitting a wake-up signal via an encrypted channel from a communication device for receipt at a remote computer.**

The step in Claim 56 of transmitting a wake-up signal comprising a network address via an encrypted communication channel to a remote computer further distinguishes this claim from *Conklin* and from *Proctor*. While *Conklin* may disclose engaging a remote system to record threatening communications and transmitting threatening communications in an encrypted format, *Conklin* does not disclose transmitting a wake-up signal via an encrypted communication

channel to a remote computer in accordance with the recitations of Claim 56. See *Conklin* column 5 lines 32-37 and column 6 lines 14-19. *Proctor* also fails to teach transmitting a wake-up signal via an encrypted communication channel to a remote computer. In contrast to such a disclosure, *Proctor* teaches revising security procedures with a security system that is on a network along with the computers to which the security procedures apply. See *Proctor* Figure 1.

D. Independent Claims 61 and 68 are Distinguishable from *Proctor* and *Conklin*

New Claim 61 is a system claim for a system that remotely monitors the security status of a plurality of computer networks, each associated with an entity, while new Claim 68 is a method claim for a method for remotely monitoring the security status of a plurality of computer networks, each associated with an entity.

Conklin and Proctor fail to disclose or teach an in-line communication device that is operative to block a communication by terminating the communication in response to a determination that the communication represents a security risk.

As discussed above in reference to Claim 41, the teachings of *Proctor* and *Conklin* contrast with blocking a communication by terminating the communication in response to a determination that the communication represents a security risk, as recited in Claims 61 and 68.

***Conklin* and *Proctor* fail to disclose or teach an in-line communication device that is operative to block a communication signal by terminating the communication signal.**

For similar reasons to those discussed above in reference to Claim 41, Claims 61 and 68 are distinguishable from *Proctor* and *Conklin* based on the recitations of an communication device coupled in-line with a computer network and a distributed computer network. Neither of these references disclose an in-line communications device in accord with Claim 61 or Claim 68.

***Conklin* and *Proctor* fail to disclose or teach a system that remotely monitors security status of a plurality of computer networks.**

As discussed above in reference to Claim 41, neither *Conklin* nor *Proctor* discloses a system that remotely monitors security status of a plurality of computer networks, as required by Claims 61 and 68.

E. Independent Claim 66 is Distinguishable from *Proctor* and *Conklin*

New Claim 66 is an independent claim for a system that remotely monitors the security status of a plurality of computer networks.

***Conklin* and *Proctor* fail to disclose or teach an in-line communication device that is operable to block a communication representing a security risk by terminating the communication.**

As described above in reference to Claim 41, the teachings of *Conklin* and of *Proctor* contrast with a communication device that is operable to block a communication by terminating the communication. Also, as discussed above, these cited references teach positioning a security system out-of-line of a network rather than teaching a communication device that is coupled in-line as defined by Claim 66.

***Conklin* and *Proctor* fail to disclose or teach a system that remotely monitors the security status of a plurality of computer networks.**

As discussed above in reference to Claim 41, the disclosures of *Proctor* and *Conklin* contrast with a system that remotely monitors the security status of a plurality of computer networks, as defined by Claim 66.

***Conklin* and *Proctor* fail to disclose or teach a remote monitoring center system having the recited features in Claim 66.**

Claim 66 recites a remote monitoring center comprising workstations operated by remote agent personnel for evaluating an alert signal, a database for storing alert information, a server for maintaining security configuration options, a controller, and a monitoring engine. In contrast to disclosing a remote monitoring center having these recited features, *Conklin* teaches

integrating security monitoring functions into existing network management systems. See *Conklin* column 1 lines 24-26. *Proctor* teaches designating one of the computers in a networked computing environment for performing network security functions. See *Proctor* column 5 lines 27-37.

F. Independent Claim 67 is Distinguishable from *Proctor* and *Conklin*

New Claim 67 is an independent claim of a communication device for intrusion protection that is coupled in-line with a computer network controlled by a user and a distributed computer network that is not controlled by the user. Applicant submits that Claim 67 is patentable over *Proctor*, *Conklin*, or a combination of *Proctor* and *Conklin,* in view of the claim recitations discussed below.

Conklin and _Proctor_ fail to disclose or teach a communication device for intrusion protection coupled in-line with a computer network and a distributed computer network.

As discussed above in reference to Claim 41, *Conklin* and *Proctor* teach positioning security systems out-of-line of a network rather than in-line as recited in Claim 67.

Conklin and _Proctor_ fail to disclose or teach an intrusion processor that is operative to block a communication from passage to a computer network, which is under control of a user, by terminating the communication in response to a determination that the communication represents a security risk.

As described above in reference to Claim 41, the teachings of *Conklin* and of *Proctor* contrast with blocking a communication representing a security risk by terminating the communication.

Conklin and _Proctor_ fail to disclose or teach an in-line communication device for intrusion protection having the recited features in Claim 67.

Claim 67 recites a communication device for intrusion protection comprising an intrusion processor for processing a communication carried by a distributed computer network and intended for delivery to a computer coupled to a computer network, a processing module

operative to determine a network address, and a transmitter for sending a wake-up signal and an alert signal to a remote monitoring center. In contrast to disclosing a communication device having these recited features, *Conklin* teaches integrating security monitoring functions into existing network management systems and coupling a security system to a network in a tap arrangement that is out-of-line with the network. See *Conklin* Figure 4 and column 1 lines 24-26. Contrary to Claim 67, *Proctor* teaches providing security system components on the same network as the computers receiving security services. See *Proctor* Figure 1.

G. Independent Claim 69 is Distinguishable from *Proctor* and *Conklin*

New Claim 69 is an independent claim for a method for remotely monitoring the security status of a plurality of computer networks, each of which is coupled to a distributed computer network and is associated with an entity. Neither *Proctor* nor *Conklin* discloses a method with the recited steps of Claim 69.

Conklin and _Proctor_ fail to disclose or teach remotely monitoring the security status of a plurality of computer networks as recited by Claim 69.

As discussed above in reference to Claim 41, *Conklin* and *Proctor* provide disclosures that contrast with remotely monitoring the security status of a plurality of computer networks.

Conklin and _Proctor_ fail to disclose or teach a step of blocking a communication from passage to a computer network by terminating the communication in response to a determination that the communication represents a security risk.

As discussed above in reference to Claim 41, the teachings of *Conklin* and of *Proctor* contrast with blocking a communication representing a security risk by terminating the communication.

Conklin and _Proctor_ fail to disclose or teach a method for remotely monitoring security status of a plurality of computer networks with the recited steps.

Claim 69 recites a method for remotely monitoring the security status of a plurality of computer networks comprising the steps of: processing a communication carried by a distributed

computer network to determine whether the communication represents a security risk; and blocking the communication from passage to the computer network by terminating the communication in response to a determination that the communication represents a security risk. The teachings of *Proctor* and *Conklin* contrast with these recited steps. In contrast to blocking a communication from passage to a network, *Conklin* teaches monitoring on the network for communications that represent a security risk. See *Conklin* Figures 1-4. Similarly, *Proctor* teaches locating a security system on a network receiving security services. See *Proctor* Figure 1.

II. New Dependent Claims 42-46, 48-55, 57-60, 62-65, and 70 are Patentable over the Cited Prior Art

In view of the foregoing remarks with respect to independent Claims 41, 47, 56, 61, and 69, Applicant respectfully submits that respective dependent Claims 42-46, 48-55, 57-60, 62-65, and 70 are patentable over *Proctor* and *Conklin*, both individually and in an alleged combination. Applicant further respectfully submits that dependent Claims 42-46, 48-55, 57-60, 62-65, and 70 are patentable over all of the references cited by the Examiner. These dependent claims recite features further defining the invention over the cited references, and Applicant submits that none of these references disclose or suggest integrating those features into the presently claimed invention. Accordingly, Applicant requests separate and individual consideration of dependent Claims 42-46, 48-55, 57-60, 62-65, and 70.